มุมนักเล่น

dBASE

ยืน ภู่วรวรรณ

การดูแลรักษาข้อมูล : แผนถล่ม มหาภัยไวรัส

ไม่ว่าเจ้าวายร้ายไวรัส
จะแอบซ่อนที่ไหน
ถ้าค้นพบล่ะก็
เราจะตามไปปราบให้สิ้น

การดูแลรักษาข้อมูลที่กล่าวมาแล้วตั้งแต่ตอนแรกของบทความชุดนี้เน้นปัญหาที่เกิดขึ้นเฉพาะระหว่างการใช้ เช่น การพลั้งเผลอในการทำงาน ปัญหาจากการไม่รู้สาเหตุ ปัญหาไฟฟ้าดับทำให้แฟ้มข้อมูลเสียหาย ความเสียหายอีกสาเหตุหนึ่งที่พบเห็นและเผชิญหน้ากันบ่อย ๆ ในขณะนี้คือปัญหาไวรัสคอมพิวเตอร์ มุมดีเบสในฉบับนี้จึงนำหลักการและแนวทางดูแลข้อมูล ตลอดจนวิธีการแก้ปัญหาที่เกิดจากไวรัสคอมพิวเตอร์

ปัญหาจากไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์ได้แพร่ระบาดออกมามากมายหลายตัว แต่ละตัวจะสร้างความเสียหายในลักษณะแตกต่างกัน ผู้ใช้หรือผู้พัฒนางานฐานข้อมูลจำเป็นต้องทำความเข้าใจ สามารถแก้ไขปัญหาอันเกิดจากไวรัสคอมพิวเตอร์ที่สำคัญ ๆ ประกอบด้วย

1. ปัญหาที่เกิดกับตารางจัดแบ่งฮาร์ดดิสค์ (hard disk partition)
2. ปัญหาที่เกิดกับบูตเซกเตอร์
3. ปัญหาที่เกิดกับ FAT
4. ปัญหาที่เกิดกับไดเรคทอรี
5. ปัญหาที่เกิดกับเซกเตอร์เก็บข้อมูลและการกำหนดให้เป็นเซกเตอร์ใช้การไม่ได้

การแก้ปัญหาแฟ้มต่าง ๆ ที่อาจเกิดขึ้นได้จึงต้องทำความเข้าใจในเรื่องรายละเอียดบางอย่างเกี่ยวกับตารางจัดแบ่งฮาร์ดดิสค์ (partition) บูตเซกเตอร์ FAT ไดเรคทอรีและเซกเตอร์เก็บข้อมูล หากเข้าใจเรื่องราวเหล่านี้ดีแล้วจะช่วยให้เราสามารถแก้ปัญหาทุกกรณีและตรวจสอบหาไวรัสเองได้

ตระกูลไวรัสบนพีซี

ไวรัสบนพีซีเป็นไวรัสคอมพิวเตอร์ที่พัฒนาให้เกาะติดอยู่ในระบบดิสค์และถ่ายลงสู่หน่วยความจำเพื่อแพร่กระจายต่อไป การยึดเหนี่ยวของไวรัสในระบบดิสค์มีสองกลุ่มคือ ไวรัสที่แอบแฝงมากับแฟ้มข้อมูลและไวรัสบนบูตเซกเตอร์หรือพาร์ติชันตารางแบ่งฮาร์ดดิสค์ ไวรัสคอมพิวเตอร์เหล่านี้จะเป็นโปรแกรมเล็ก ๆ ซุกซ่อนตัวในตำแหน่งต่าง ๆ ของดิสค์ โดยอาศัยการโหลดของระบบเพื่อเล็ดลอดเข้าไปในหน่วยความจำ ซึ่งเป็นแหล่งที่อยู่อาศัยที่เหมาะสมโดยแทรกตัวเข้าไปในบูตเซกเตอร์ ไฟล์

ประเภท .COM, .EXE หรือแม้แต่ไฟล์ประเภทโอเวอร์เลย์ .OVR เพราะไฟล์เหล่านี้มีโอกาสเรียกลงในหน่วยความจำ

ไวรัสชนิดเกาะไฟล์

ไวรัสที่ติดอยู่กับไฟล์นี้เป็นโปรแกรมที่รวมเข้าไปกับโปรแกรม .COM หรือ .EXE เมื่อเราเรียกไฟล์เหล่านี้ ไวรัสจะแยกไปซ่อนตัวอยู่ในหน่วยความจำที่ใดที่หนึ่ง แล้วหาทางคัดลอกตัวเองประกบติดแฟ้มประเภท .EXE และ .COM ที่เก็บไว้ในดิสค์อื่น ๆ อีก ไวรัสจำพวกนี้อาจเกาะตอนท้ายหรือตอนต้นไฟล์ ดังนั้นจึงทำให้ขนาดของแฟ้มข้อมูลที่มีไวรัสโตขึ้น ยิ่งเป็นไวรัสคอมพิวเตอร์ที่เกาะติดได้หลายครั้ง เมื่อขนาดของไฟล์เพิ่มขึ้นเรื่อย ๆ ในที่สุดเราอาจไม่สามารถโหลดไฟล์นั้นลงในหน่วยความจำ

ไวรัสที่บูตเซกเตอร์หรือพาร์ติชันแบ่งฮาร์ดดิสค์

ไวรัสประเภทนี้จะมีเพียงบางส่วนอยู่ในเซกเตอร์พาร์ติชันแบ่งฮาร์ดดิสค์ บางตัวอยู่ที่บูตเซกเตอร์ ดังนั้นทุกครั้งที่บูตระบบไวรัสจะถูกโหลดเข้าไปหลบซ่อนในหน่วยความจำ เพื่อแพร่กระจายต่อไปยังดิสค์หรือดิสเกตต์แผ่นอื่น ไวรัสบางตัวในส่วนของพาร์ติชันจะฝังตัวบนดิสค์ได้ดี เพราะการฟอร์แมตฮาร์ดดิสค์ใหม่ด้วยวิธีของดอสไม่สามารถลบและจัดการทำลายไวรัสประเภทนี้ได้โดยตรง นอกเสียจากว่าเราจะต้องทำการฟอร์แมตระดับล่างที่เรียกว่าพรีฟอร์แมต ซึ่งผู้ดำเนินการควรเข้าใจวิธีการฟอร์แมตด้วย

เพื่อให้สถานการณ์การใช้งานของเราปลอดจากไวรัสคอมพิวเตอร์ และสามารถแก้ไขปัญหาหลาย ๆ อย่างด้วยตนเอง ในที่นี้ผู้เขียนได้เสริมความรู้ในเรื่องต่าง ๆ เพื่อให้ทราบแนวทางใช้งาน ป้องกัน แก้ไข หรือทำลายไวรัสคอมพิวเตอร์ในโอกาสต่อไป

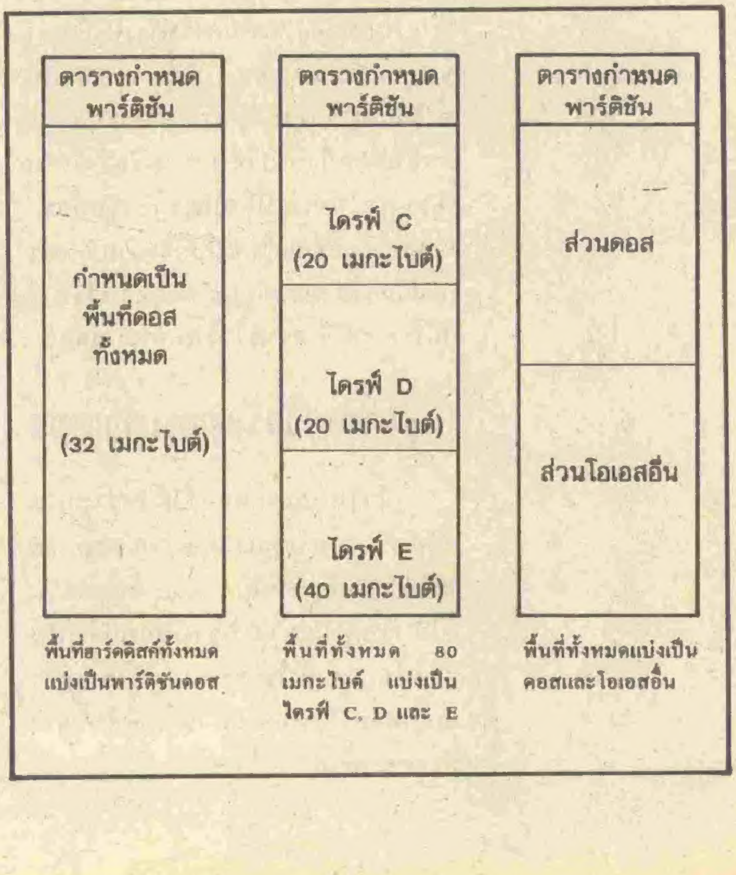
รู้จักกับตารางพาร์ติชัน

ในฮาร์ดดิสค์แต่ละไดรฟ์จะประกอบด้วยแผ่นดิสค์หลายแผ่นวางซ้อนกัน ฮาร์ดดิสค์แต่ละตัวจะมีหลายไซด์ จำนวนเท่ากับหัวอ่านฮาร์ดดิสค์ในแต่ละหน้าของการเก็บข้อมูล โดยแบ่งเป็นไซลินเดอร์ แต่ละไซลินเดอร์จะแบ่งเป็นเซกเตอร์ เราจะเรียกว่าเซกเตอร์แบบแอ็บโซลุต เช่น ฮาร์ดดิสค์ไดรฟ์หนึ่งอาจแบ่งออกเป็นไดรฟ์ย่อย C และ D (เมื่อใช้งาน) การแบ่งรายละเอียดฮาร์ดดิสค์นี้จะต้องกระทำก่อนการฟอร์แมตฮาร์ดดิสค์

จุดมุ่งหมายของการแบ่งพาร์ติชันก็เพื่อให้แบ่งเป็นไดรฟ์ย่อย C: D: E: หรือแบ่งพื้นที่เพื่อใช้งานหลายโอเอส เช่น ใช้กับดอส ซีนิกซ์ หรือโอเอสอื่น ตารางพาร์ติชันนี้จะเป็นตัวกำหนดรายละเอียดการแบ่ง โครงสร้างฮาร์ดดิสค์อาจแบ่งแยกเป็นส่วน ๆ ได้ดังรูปที่ 1

ข้อมูลตารางพาร์ติชันอยู่ไหน

ผู้ใช้งานฮาร์ดดิสค์ในระบบดอสไม่สามารถเรียกเข้าไปยังส่วนภายนอกพื้นที่ที่ฟอร์แมตด้วยดอส หรือกล่าวอีกนัยหนึ่ง ดอสจะอ้างอิงออกนอกกรอบของพื้นที่ที่ดอสกำหนดไว้ไม่ได้ การติดตั้งฮาร์ดดิสค์ครั้งแรกจะต้องแบ่งพาร์ติชันด้วยการใช้โปรแกรม FDISK และสร้างพาร์ติชันของดอส ผู้ใช้งานจึงควรรู้จักหน้าตาพาร์ติชันของดิสค์ตนเองไว้ เผื่อว่าถ้าหากไวรัสคอมพิวเตอร์แอบแก้ข้อมูลพาร์ติชัน เราจะได้ทราบและสามารถแก้ไขกลับคืนได้ เช่น บางครั้งการใช้งานของเราเป็นไดรฟ์ C อยู่ ๆ ชื่อไดรฟ์เปลี่ยนไปเป็นไดรฟ์ D ซึ่งอาจเกิดจากไวรัสคอมพิวเตอร์เป็นต้นเหตุ



พื้นที่ฮาร์ดดิสค์ทั้งหมดแบ่งเป็นพาร์ติชันดอส

พื้นที่ทั้งหมด 80 เมกะไบต์ แบ่งเป็นไดรฟ์ C, D และ E

พื้นที่ทั้งหมดแบ่งเป็นดอสและโอเอสอื่น

รูปที่ 1
การแบ่งพาร์ติชันของฮาร์ดดิสค์

ข้อมูลในส่วนพาร์ติชันนี้ไม่ควรจะเปลี่ยนแปลงเองได้

หากต้องการดูว่าข้อมูลพาร์ติชันของดิสค์ที่ใช้อยู่เป็นอย่างไร ให้ใช้ยูทิลิตี้ในการซ่อมไฟล์หรือข้อมูลในดิสค์ เช่น นอร์ตันยูทิลิตี้ (Norton Utility) โดยทำตามขั้นตอนดังนี้

1. เรียก NU จากนั้นเลือก Explore disk
2. เลือก absolute sector
3. เลือกส่วนตารางพาร์ติชันซึ่งอยู่ในไซด์ 0 ไซลินเดอร์ 0 เซกเตอร์ 1 และจำนวนเซกเตอร์จะใช้เท่าไรก็ได้
4. จากนั้นเลือก Edit/Display item

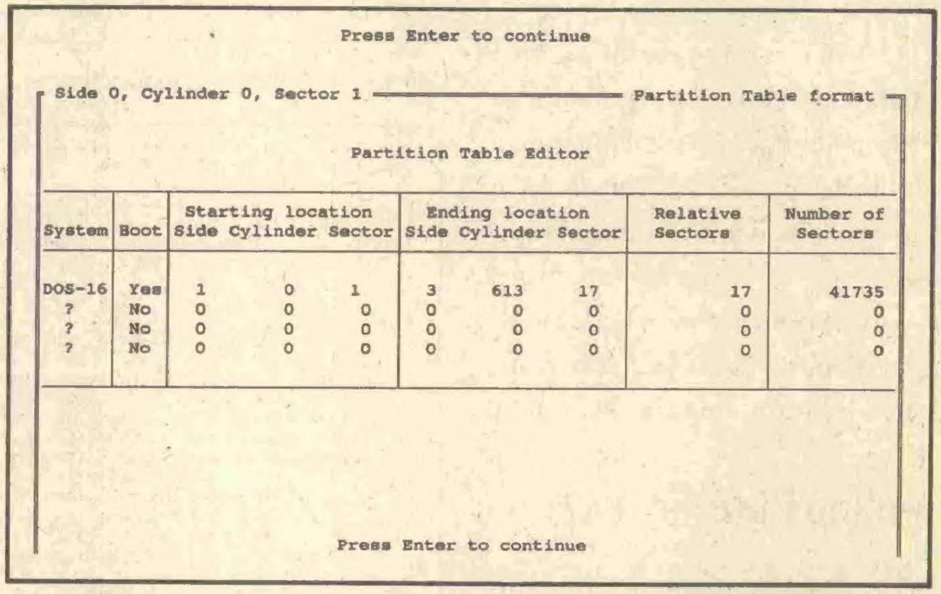
ผลที่ได้บนจอภาพเป็นดังรูปที่ 2 สำหรับข้อมูลจัดแบ่งส่วนดิสค์ที่เก็บไว้นี้มีความสำคัญมาก จากข้อมูลดังกล่าวสรุปได้ว่า ฮาร์ดดิสค์นั้นเก็บดอสเป็นพาร์ติชันแรก โดยดอสตั้งแต่หน้า 1 ไซลินเดอร์ 0 เซกเตอร์ 1 ไปจนหมดดิสค์ ทั้งหมดเป็นจำนวน 41736 นั่นคือ ด้วย 0 หรือไซด์ 0 ไซลินเดอร์ 0 เป็นส่วนที่ดอสมองไม่เห็น ไวรัสอาจหลบอยู่ในนี้ได้ การฟอร์แมตด้วยดอสจะไม่สามารถกระทำกับส่วนข้อมูลในพาร์ติชัน หากมีการแก้ไขจะทำให้เกิดปัญหาเช่นกัน ดังนั้นเราควรระวังให้ดี ถ้าไม่แน่ใจอย่าเขียนข้อมูลใด ๆ ลงในบริเวณนี้ มิฉะนั้นฮาร์ดดิสค์จะเสียหายทั้งหมด

เมื่อพิจารณาข้อมูลแบบตัวเลขฐานสิบหก ผลของข้อมูลพาร์ติชันจะเป็นดังรูปที่ 3

สิ่งสำคัญอย่างหนึ่งคือ พยายามจดจำข้อมูลของพาร์ติชันฮาร์ดดิสค์ไว้เสมอ เพราะหากเกิดการเปลี่ยนแปลงไปจากเดิมที่เป็นอยู่ เราจะได้ทราบทันที และหาทางแก้ไขเพื่อให้ได้ผลที่ต้องการกลับคืนมา ข้อมูลในพาร์ติชันนี้ยังต่อเนื่องได้อีกหลายเซกเตอร์ ในกรณีนี้จะมีจนถึง 17 เซกเตอร์ ดังนั้นในไซด์ 0 ไซลินเดอร์ 0 ทั้ง 17 เซกเตอร์เป็นพื้นที่ขนาดใหญ่พอที่ข้อมูลไวรัสจะซ่อนอยู่ ลองตรวจหาด้วย NU โดยปกติจะพบตัวเลข 0 ว่างเปล่าหรือกล่าวได้ว่าไม่มีข้อมูลแปลกปลอมใด ๆ

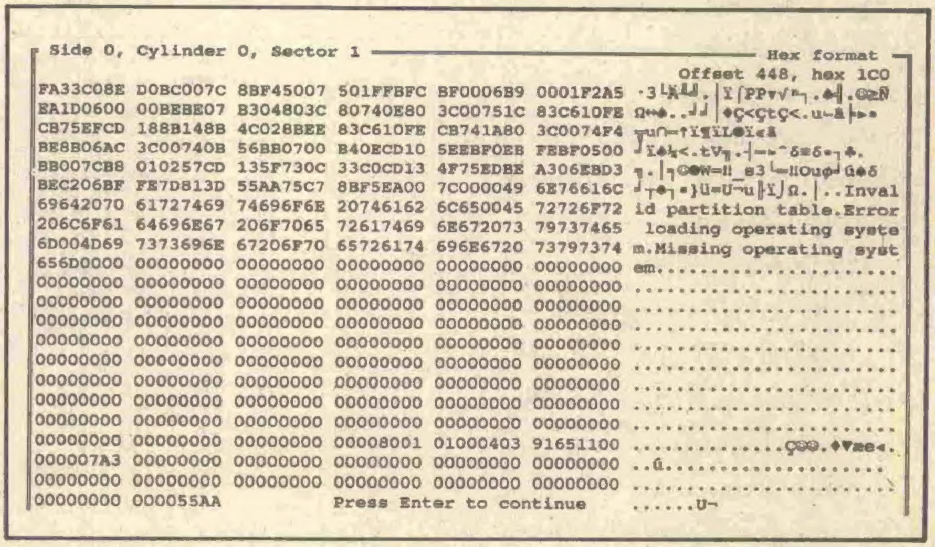
บูตเซกเตอร์

บริเวณบูตเซกเตอร์เป็นอีกส่วนหนึ่งที่ควรจะรู้จัก ใช้สำหรับเก็บข้อมูลและโปรแกรมสำหรับโหลดดอสลงสู่หน่วยความจำ โดยทำหน้าที่อ่านและนำโปรแกรมบูตไว้ในหน่วยความจำเสมอทุกครั้งที่ต้องการบูตดอส บูตเซกเตอร์ของฟลอปปี้ดิสค์จะอยู่ที่ไซด์ 0 ไซลินเดอร์ 0



```
                         Press Enter to continue

 Side 0, Cylinder 0, Sector 1 ────────────────── Partition Table format

                         Partition Table Editor

               Starting location       Ending location        Relative     Number of
System  Boot  Side Cylinder Sector  Side Cylinder Sector      Sectors       Sectors

DOS-16  Yes    1       0       1     3     613     17              17         41735
  ?     No     0       0       0     0       0      0               0             0
  ?     No     0       0       0     0       0      0               0             0
  ?     No     0       0       0     0       0      0               0             0

                         Press Enter to continue
```

รูปที่ 2 ผลบนจอภาพหลังจากเสร็จสิ้นขั้นตอนการใช้ NU เพื่อการซ่อมไฟล์หรือข้อมูลในดิสค์

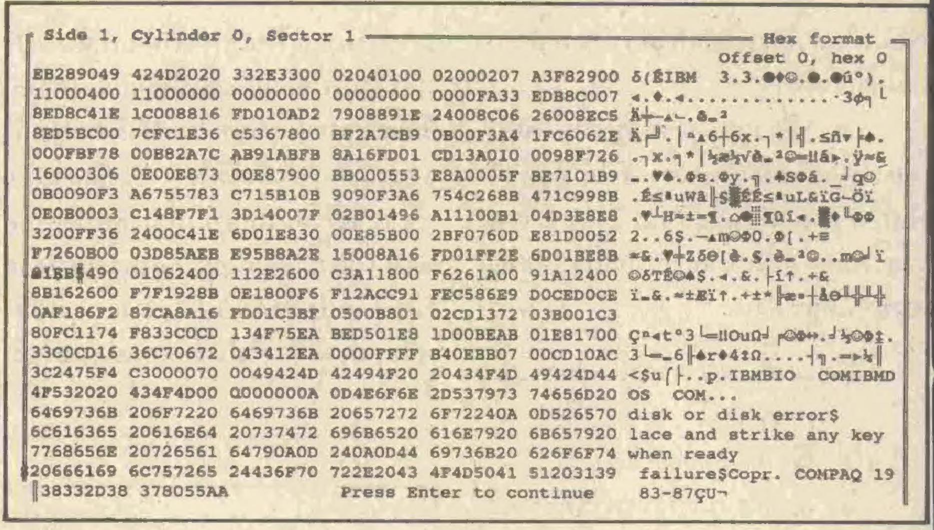


```
 Side 0, Cylinder 0, Sector 1 ───────────────────────────────────── Hex format
                                                          Offset 448, hex 1C0
FA33C08E D0BC007C 8BF45007 501FFBFC BF0006B9 0001F2A5 ·3└Ä╚╝.│ï⌠PP▼√┐ⁿ┐.♠╢.ⁿ≥Ñ
EA1D0600 00BEBE07 B304803C 80740E80 3C00751C 83C610FE Ω↔♠..╛╛│♦Ç<Çt♫Ç<.u∟â╞►■
CB75EFCD 188B148B 4C028BEE 83C610FE CB741A80 3C0074F4 ╦u∩═↑ï¶ïL☻ïεâ╞
BE8B06AC 3C00740B 56BB0700 B40ECD10 5EEBF0EB FEBF0500 ╛ï♠¼<.t♂V╗•.┤♫═►^δ≡δ■┐♣.
BB007CB8 010257CD 135F730C 33C0CD13 4F75EDBE A306EBD3 ╗.│╕☺☻W═‼_s♀3└═‼Ouφ╛ú♠δ╙
BEC206BF FE7D813D 55AA75C7 8BF5EA00 7C000049 6E76616C ╛┬♠┐■}ü=U¬u╟ï⌡Ω.│..Inval
69642070 61727469 74696F6E 20746162 6C650045 72726F72 id partition table.Error
206C6F61 64696E67 206F7065 72617469 6E672073 79737465  loading operating syste
6D004D69 7373696E 67206F70 65726174 696E6720 73797374 m.Missing operating syst
656D0000 00000000 00000000 00000000 00000000 00000000 em......................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 00000000 00000000 00008001 01000403 91651100 ..............Ç☺☺.♦♥æe◄.
000007A3 00000000 00000000 00000000 00000000 00000000 ..ú.....................
00000000 00000000 00000000 00000000 00000000 00000000 ........................
00000000 000055AA          Press Enter to continue    ......U¬
```

รูปที่ 3 ผลของข้อมูลพาร์ติชันแบบตัวเลขฐานสิบหก

ของเซกเตอร์ 1 แต่กรณีของฮาร์ดดิสค์บูตเซกเตอร์อาจแตกต่างกันไปตามส่วนของการแบ่งพาร์ติชัน ซึ่งจะขึ้นกับพาร์ติชันดอสที่แอคตีฟ เพื่อว่าเวลาเปิดเครื่องจะดูจากพาร์ติชันก่อน เมื่อทราบตำแหน่งบูตแล้วค่อยอ่านบูตเซกเตอร์ที่กำหนด

ตัวอย่างที่หยิบยกให้ดูนี้เป็นฮาร์ดดิสค์ที่มีบูตเซกเตอร์อยู่ที่ 0 ไซด์ 1 ไซลินเดอร์ 0 เซกเตอร์ 1 ผลที่ได้เมื่อใช้ NU คือรูปที่ 4



```
Side 1, Cylinder 0, Sector 1 ──────────────────────── Hex format
                                                     Offset 0, hex 0
EB289049 424D2020 332E3300 02040100 02000207 A3F82900 δ(ÊIBM  3.3.●♦☺.●.●ú°).
11000400 11000000 00000000 00000000 0000FA33 EDB8C007 ◄.♦.◄...............·3φ╕└
8ED8C41E 1C008816 FD010AD2 7908891E 24008C06 26008EC5 Ä┼─▲∟.ê▬²
8ED5BC00 7CFC1E36 C5367800 BF2A7CB9 0B00F3A4 1FC6062E Ä╒╝.|ⁿ▲6┼6x.┐*|╣.≤ñ▼╞♠.
000FBF78 00B82A7C AB91ABFB 8A16FD01 CD13A010 0098F726 .┐x.╕*|½æ½√è▬²☺═‼á►.ÿ≈&
16000306 0E00E873 00E87900 BB000553 E8A0005F BE7101B9 ▬.♥♠.Φs.Φy.╗.♣SΦá._╛q☺╣
0B0090F3 A6755783 C715B10B 9090F3A6 754C268B 471C998B .É≤ªuWâ╟§▒ÉÉ≤ªuL&ïG∟Öï
0E0B0003 C148F7F1 3D14007F 02B01496 A11100B1 04D3E8E8 .♂.♥┴H≈±=¶.⌂☻░¶ûí◄.▒♦╙ΦΦ
3200FF36 2400C41E 6D01E830 00E85B00 2BF0760D E81D0052 2..6$.─▲m☺Φ0.Φ[.+≡v.Φ↔.R
F7260B00 03D85AEB E95B8A2E 15008A16 FD01FF2E 6D01BE8B ≈&.♥╪ZδΘ[è.§.è▬²☺..m☺╛ï
A1EB$490 01062400 112E2600 C3A11800 F6261A00 91A12400 ☺δTÉ☺♠$.◄.&.├í↑.÷&→.æí$.
8B162600 F7F1928B 0E1800F6 F12ACC91 FEC586E9 D0CED0CE ï▬&.≈±Æï♫↑.÷±*╠æ■┼åΘ╨╬╨╬
0AF186F2 87CA8A16 FD01C3BF 0500B801 02CD1372 03B001C3
80FC1174 F833C0CD 134F75EA BED501E8 1D00BEAB 01E81700 Çⁿ◄t°3└═‼OuΩ╛╒☺Φ↔.╛½☺Φ↨.
33C0CD16 36C70672 043412EA 0000FFFF B40EBB07 00CD10AC 3└═▬6╟♠r♦4↕Ω....┤♫╗•.═►¼
3C2475F4 C3000070 0049424D 42494F20 20434F4D 49424D44 <$u⌠├..p.IBMBIO  COMIBMD
4F532020 434F4D00 0000000A 0D4E6F6E 2D537973 74656D20 OS  COM...
6469736B 206F7220 6469736B 20657272 6F72240A 0D526570 disk or disk error$
6C616365 20616E64 20737472 696B6520 616E7920 6B657920 lace and strike any key
7768656E 20726561 64790A0D 240A0D44 69736B20 626F6F74 when ready
20666169 6C757265 24436F70 722E2043 4F4D5041 51203139  failure$Copr. COMPAQ 19
38332D38 378055AA            Press Enter to continue    83-87ÇU¬
```

รูปที่ 4 ฮาร์ดดิสค์ที่มีบูตเซกเตอร์เมื่อเรียกดูด้วย NU

อนึ่ง ผู้ใช้ควรจดจำข้อมูลของบูตเซกเตอร์ไว้ หากเกิดการเปลี่ยนแปลงไปจากเดิมแสดงว่ามีไวรัสหรือโปรแกรมแปลกปลอม อย่างไรก็ตาม ข้อมูลในบูตเซกเตอร์จะแตกต่างกันขึ้นกับเวอร์ชันของดอส โดยตัวฟอร์แมตจะสร้างให้ ดังนั้นการฟอร์แมตแผ่นดิสค์ด้วยดอสเวอร์ชันเดียวกันจะได้ข้อมูลบนบูตเซกเตอร์เหมือนกันเซกเตอร์ต่อมาคือ FAT

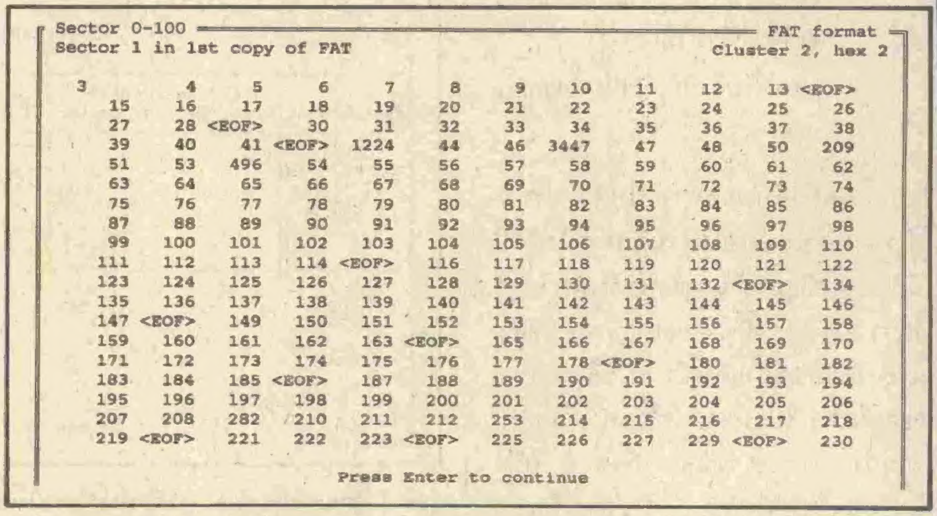
เซกเตอร์ต่อมาคือ FAT

ข้อมูลที่เก็บในดิสค์เซกเตอร์ถัดจากบูตจะเป็น FAT โดยปกติจะมี FAT สองชุด เพื่อกันข้อผิดพลาดหรือสร้างความน่าเชื่อถือให้ข้อมูล หากต้องการดูข้อมูล FAT ให้เลือก NU แล้วเข้า Explore disk เลือก Sector กำหนดเซกเตอร์ในส่วนของ FAT ในกรณีนี้จะเริ่มจาก 1 เป็นต้นไป

ผลของข้อมูล FAT ชุดที่ 1 เมื่อเรียก Edit/Display จะได้ดังรูปที่ 5

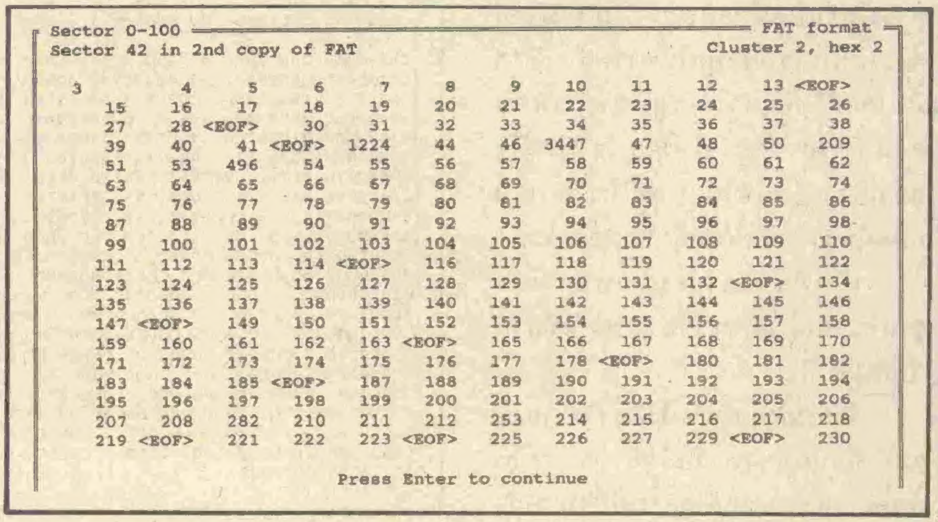
เมื่อเรียก FAT ชุดที่ 2 ซึ่งในที่นี้เริ่มจากเซกเตอร์ 42 ผลของการอ่านด้วย NU จะแสดงได้ดังรูปที่ 6

ข้อควรสังเกต FAT ที่เก็บไว้บนดิสค์จะมีสองชุด ดังนั้นหากพบปัญหาจาก FAT ชุดที่ 1 ให้นำข้อมูลในชุดที่สอง



```
Sector 0-100 ══════════════════════════════════════════ FAT format
Sector 1 in 1st copy of FAT                          Cluster 2, hex 2

  3        4     5     6     7     8     9    10    11    12    13 <EOF>
     15   16    17    18    19    20    21    22    23    24    25    26
     27   28 <EOF>    30    31    32    33    34    35    36    37    38
     39   40    41 <EOF>  1224    44    46  3447    47    48    50   209
     51   53   496    54    55    56    57    58    59    60    61    62
     63   64    65    66    67    68    69    70    71    72    73    74
     75   76    77    78    79    80    81    82    83    84    85    86
     87   88    89    90    91    92    93    94    95    96    97    98
     99  100   101   102   103   104   105   106   107   108   109   110
    111  112   113   114 <EOF>   116   117   118   119   120   121   122
    123  124   125   126   127   128   129   130   131   132 <EOF>   134
    135  136   137   138   139   140   141   142   143   144   145   146
    147 <EOF>  149   150   151   152   153   154   155   156   157   158
    159  160   161   162   163 <EOF>   165   166   167   168   169   170
    171  172   173   174   175   176   177   178 <EOF>   180   181   182
    183  184   185 <EOF>   187   188   189   190   191   192   193   194
    195  196   197   198   199   200   201   202   203   204   205   206
    207  208   282   210   211   212   253   214   215   216   217   218
    219 <EOF>  221   222   223 <EOF>   225   226   227   229 <EOF>   230

                          Press Enter to continue
```

รูปที่ 5 ผลของข้อมูล FAT ชุดที่ 1 หลังจากเรียก Edit/Display



```
Sector 0-100 ══════════════════════════════════════════ FAT format
Sector 42 in 2nd copy of FAT                         Cluster 2, hex 2

  3        4     5     6     7     8     9    10    11    12    13 <EOF>
     15   16    17    18    19    20    21    22    23    24    25    26
     27   28 <EOF>    30    31    32    33    34    35    36    37    38
     39   40    41 <EOF>  1224    44    46  3447    47    48    50   209
     51   53   496    54    55    56    57    58    59    60    61    62
     63   64    65    66    67    68    69    70    71    72    73    74
     75   76    77    78    79    80    81    82    83    84    85    86
     87   88    89    90    91    92    93    94    95    96    97    98
     99  100   101   102   103   104   105   106   107   108   109   110
    111  112   113   114 <EOF>   116   117   118   119   120   121   122
    123  124   125   126   127   128   129   130   131   132 <EOF>   134
    135  136   137   138   139   140   141   142   143   144   145   146
    147 <EOF>  149   150   151   152   153   154   155   156   157   158
    159  160   161   162   163 <EOF>   165   166   167   168   169   170
    171  172   173   174   175   176   177   178 <EOF>   180   181   182
    183  184   185 <EOF>   187   188   189   190   191   192   193   194
    195  196   197   198   199   200   201   202   203   204   205   206
    207  208   282   210   211   212   253   214   215   216   217   218
    219 <EOF>  221   222   223 <EOF>   225   226   227   229 <EOF>   230

                          Press Enter to continue
```

รูปที่ 6 ผลของการอ่าน FAT ชุดที่ 2 ด้วย NU

คัดลอกลงไปแทน ข้อมูลของ FAT จะช่วยให้เราซ่อมแซมแก้ไขแฟ้มข้อมูลที่เป็นปัญหาได้ดังที่กล่าวข้างต้น

การตรวจแฟ้มข้อมูลด้วย .COM หรือ .EXE

การตรวจแฟ้มข้อมูลด้วย NU กระทำได้ง่าย เริ่มด้วยการเลือก Explore disk จากนั้นเลือก item ที่เป็น file เลือกชื่อไฟล์ที่ต้องการ แล้วใช้ Edit/Display เพื่อดูรายละเอียดข้อมูลในไฟล์ ส่วนใหญ่จะเป็นไบนารีไฟล์และยากที่จะรู้ได้ว่าคืออะไร

หากต้องการตรวจสอบว่ามีไวรัสติดอยู่หรือไม่ เราใช้วิธีการเปรียบเทียบถ้ามีไฟล์โปรแกรมต้นฉบับบนดิสเกตต์และมั่นใจว่าไม่มีไวรัส เช่น NC.EXE กับ NC.EXE ไฟล์บนฮาร์ดดิสค์ที่คิดว่ามีไวรัส ซึ่งจะแตกต่างกันตรงที่ขนาดของแฟ้มหรือมีข้อน่าสงสัยอื่น ให้ใช้ NU อ่านไฟล์ แล้วเปรียบเทียบความแตกต่าง ข้อแตกต่างของทั้งสองไฟล์นี้คือตัวไวรัสล่ะ

การตรวจสอบกรณีที่สงสัยว่ามีไวรัสนี้ ควรจะนำแผ่นดิสเกตต์ที่ต้องการตรวจติดการป้องกันเขียนไว้ด้วย มิฉะนั้นอาจจะมีไวรัสเข้าไปเกาะขณะกำลังตรวจสอบก็ได้

พลิกไฟล์หาไวรัส

ปัจจุบันมีผู้พัฒนาโปรแกรมสแกนหาไวรัสขึ้นมาหลายตัว แต่โปรแกรมที่คิดว่าใช้ได้ผลดีมากคือ VIRSCAN ของบริษัทไอบีเอ็ม โดยการสแกนหาตามลายเซ็นไวรัสที่กำหนดไว้ในไฟล์เอกสารสองไฟล์คือ SIGBOOT.LST และ SIGFILE.LST

ลายเซ็นไวรัสคอมพิวเตอร์หรือ SIGNATURE หมายถึงข้อมูลที่เรียงกันกลุ่มหนึ่งที่มีลักษณะเด่นชัดบอกถึงไวรัสคอมพิวเตอร์ตัวนั้น ๆ การดูลายเซ็นนี้อาจตรวจได้จากการค้นหาว่าไวรัสเกาะอยู่ที่ใด และมีข้อมูลตัวเลขฐานสิบหกตรงไหนบ้างที่คิดว่าเป็นไวรัสแน่นอน กรณีไวรัสจะพบว่าไฟล์ทุกไฟล์ที่มีไวรัสเกาะจะมีลายเซ็นนี้เสมอ

เช่นตัวอย่างไวรัสที่ชื่อ KEY PRESS เกาะบนไฟล์ทั้ง .COM และ .EXE เมื่อตรวจสอบข้อมูลส่วนไวรัสที่พอเก็บเป็นลายเซ็นได้ดังนี้

```
C32E434F3D002E45584500068E0629018
BFA32COB98000FC
```

เมื่อได้ลายเซ็นนี้แล้วอยากเพิ่มใน SIGFILE.LST เพื่อให้โปรแกรม VIRSCAN ตรวจสอบไวรัสนี้ต่อไป เราทำได้โดยใช้เอดิเตอร์เรียกไฟล์ SIGFILE.-LST เพื่อเพิ่มข้อมูลเหล่านี้คือ

```
        C32E434F3D002E45584500068
        E0629018BFA32COB98000FC
      This file may be infected with the
              "Keypress VIRUS"
            (COM and EXE files)
```

เมื่อเก็บข้อมูลลง SIGFILE.LST หลังจากนั้นเวลาใช้ VIRSCAN จะทำให้เราค้นหาไวรัสตัวนี้ได้ ดังนั้นเราจึงสามารถเพิ่มเติมลายเซ็นไวรัสต่าง ๆ ได้

จัดการกับไวรัส

หากผู้อ่านเข้าใจเรื่องพาร์ติชัน บูตเซกเตอร์ หรือวิธีการแก้ไขเปลี่ยนแปลงข้อมูลได้ชัดเจน ปัญหาไวรัสก็เป็นเรื่องง่าย หากพบไวรัสบนพาร์ติชันก็จัดการเปลี่ยนแปลงข้อมูลให้กลับสภาพเดิม ถ้าพบที่บูตแก้ไขได้ด้วยการเปลี่ยนแปลงบูตเซกเตอร์ใหม่ หรือเมื่อพบไวรัสที่ไฟล์เพียงลบไฟล์นั้นทิ้งไปแล้วนำ .EXE หรือ .COM ที่ทำสำเนาหลักเก็บไว้มาโหลดใหม่ การต่อสู้กับไวรัสจึงต้องมีสำเนาโปรแกรม .COM และ .EXE ที่เป็นมาสเตอร์ หากพบที่ฮาร์ดดิสค์จากการสแกนตรวจสอบจากการสแกนจะใช้วิธีลบทิ้งแล้วโหลดตัวใหม่ลงไป

ครั้นไวรัสจู่โจมทำลายข้อมูล โดยเฉพาะการทำลายบางส่วนของดิสค์ การตรวจสอบและแก้ไขข้อมูลจะต้องกระทำด้วยความระมัดระวังและความเข้าใจในโครงสร้างของดิสค์ เชื่อได้ว่าจะเป็นประโยชน์ต่อการแก้ไขปัญหาอย่างมาก

ส่งท้าย

ภารกิจการต่อสู้ไวรัสคอมพิวเตอร์และการดูแลรักษาข้อมูลในยุคไมโครคอมพิวเตอร์เฟื่องฟูคงจะต้องปลูกฝังความรับผิดชอบร่วมกัน ผู้เขียนหวังว่าแนวทางและบทความนี้คงจะเป็นประโยชน์ต่อผู้ใช้ไมโครคอมพิวเตอร์ในอันที่จะลดปัญหาที่เกิดขึ้น ส่งผลให้การใช้ไมโครคอมพิวเตอร์ประสบผลสำเร็จตามวัตถุประสงค์ จึงขออวยพรให้ผู้อ่านทุกคนปราบไวรัสคอมพิวเตอร์ และโชคดีกับการใช้คอมพิวเตอร์ตลอดไป